STOP.THINK.CONNECT.™

Department of Homeland Security Federal Government Offerings, Products, and Services

The Department of Homeland Security (DHS) partners with the public and private sectors to improve the cybersecurity of the Nation's critical infrastructures by facilitating risk management activities that reduce cyber vulnerabilities and minimize cyber attacks.

PARTNERSHIP OPPORTUNITIES

The **Critical Infrastructure Partnership Advisory Council (CIPAC)** is a partnership between government and critical infrastructure owners and operators, which provides a forum to engage in a broad spectrum of critical infrastructure protection activities, like the Cross-Sector Cyber Security Working Group. To learn more, email cipac@dhs.gov.

The **Information Technology-Government Coordinating Council (IT-GCC)** brings together diverse Federal, state, local and tribal interests to identify and develop collaborative strategies that advance IT critical infrastructure protection.
The IT-GCC serves as a counterpart to the IT-Sector Coordinating Council (IT-SCC).

The **Federal CISO Advisory Council** provides a trusted forum for collaboration amongst the Federal CISO community. The Advisory Council champions affinity groups to share experiences and collective expertise regarding the implementation of key cybersecurity capabilities which supports the ultimate goal of facilitating enhancements to the overall cybersecurity posture of the federal government. For more information, contact FISMA.FNS@dhs.gov.

The **Industrial Control Systems Joint Working Group** facilitates information sharing between the Federal Government and private sector owners and operators in all critical infrastructure sectors in an effort to reduce the risk of cyber threats to the Nation's Industrial Control Systems. For more information, contact icsjwg@dhs.gov.

The **International Affairs Program (IAP)** partners with international entities to enhance information sharing, increase situational awareness, improve incident response capabilities, and coordinate strategic policy issues. The IAP participates in a number of forums, including the Asia Pacific Economic Cooperation (APEC), Organization of American States (OAS), International Telecommunication Union (ITU), the Organization of Economic Cooperation and Development (OECD), and the Meridian Process. For more information, contact NCSDinternationalaffairs2@hg.dhs.gov.

CYBER ASSESSMENTS, EVALUATIONS, AND REVIEWS

The Supply Chain Risk Management (SCRM) Program has a comprehensive set of **Supply Chain Management Technical Risk Assessments** tailored to department and agency needs, to include; destructive and non-destructive analysis; code review and assessment; development of attack graphs, vulnerability assessments, and mitigation recommendations. SCRM also performs **Acquisition Threat and Risk Assessments**, which allow department and agency program managers to submit system acquisition requirements for review in exchange for risk assessment reports on competing vendors.

The SCRM Program's **Incident Response and SCRM Analysis** capabilities, include analyzing vulnerabilities in Information and Communications Technology (ICT) products and systems to provide a broad view into the types of threats and vulnerabilities faced by departments and agencies. To learn more about SCRM, contact DHS_SCRM@dhs.gov.

The **Cyber Security Evaluation Tool (CSET)** provides a systematic and repeatable approach to assess the cybersecurity posture of ICS networks. CSET is a stand-alone software tool that enables users to assess their network and ICS security practices against industry and government standards and it provides prioritized recommendations. To request a CSET CD, email cset@dhs.gov. For all other questions, email cssp@dhs.gov or visit http://www.us-cert.gov/control_systems/.

The **Cybersecurity Assessment and Risk Management Approach (CARMA)** assists public and private sector partners assess, prioritize, and manage cyber infrastructure risk by providing a picture of sector-wide risks for different categories of cyber critical infrastructure. For more information, email NCSD_CIP-CS@dhs.gov.

Cybersecurity Compliance Validations (CCV) assessments are conducted collaboratively with an agency and incorporate data collection and analysis, staff interviews, and direct observation to measure and validate federal agency progress implementing capabilities and meeting requirements stemming from the Comprehensive National Cybersecurity Initiative (CNCI), the Trusted Internet Connections (TIC) Initiative, FISMA, and Office of Management and Budget guidance and, optionally, to assess Network Operations Center (NOC)/Security Operations Center (SOC) maturity. CCV assessments utilize an objective, repeatable, and consistent methodology to ensure fairness and facilitate federal-wide trending and analysis.

Risk and Vulnerability Assessments (RVA) are one-on-one engagements with agencies that combine national level threat and vulnerability information and data collected and discovered through the agency assessment, to provide agency specific risk analysis reports with strategic remediation recommendations prioritized by risk. Service capabilities include network (wired and wireless) mapping and system characterization, vulnerability scanning and validation, threat identification and evaluation, application/database/operating system configuration review and NOC/SOC response testing.

CCV and RVA assessments provide agencies with access to specialized skills and services that promote a healthy IT infrastructure across the nation's computer networks and systems. For more information, or to request services, visit http://www.dhs.gov/xabout/structure/gc_1279040901927.shtm or contact FNS.CAP_INFO@hq.dhs.gov.

Program Maturity Evaluation and the **Security Management Maturity Questionnaire (SMMQ)** is derived from the Carnegie Mellon CERT Resilience Management Model (CERT-RMM) and provides a tool agencies can use to assess their processes, identify and manage risks to key assets, and evaluate organizational maturity of their security risk management program. The SMMQ is available as a questionnaire-based assessment instrument. For more information, contact FNS.SM@dhs.gov.

EDUCATION AND WORKFORCE DEVELOPMENT INITIATIVES

DHS and the National Security Agency (NSA) co-sponsor the **National Centers of Academic Excellence** in Information Assurance Education (CAE/IA), CAE-Research (CAE-R), and the two-year (CAE2Y) programs, which promote higher education in cybersecurity and produce growing numbers of IA workers. For more information, visit http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

DHS and the National Science Foundation offer the **Scholarship for Service Program (SFS)** to outstanding undergraduate, graduate, and doctoral students in exchange for government service at a Federal agency. SFS is building a strong pipeline of skilled employees to fill critical IA positions. For more information, see https://www.sfs.opm.gov.

The **Federal Virtual Training Environment (FedVTE)** provides online access to more than 800 hours of classroom training and 75 hands-on labs to more than 125,000 Federal employees. Contact FedVTE@dhs.gov for more information.

The **Federal Cybersecurity Training Exercise (FedCTE)** provides interactive events that bring Federal participants together to share cybersecurity best practices in a secure, simulated environment. Contact FedCTE@dhs.gov for more information.

SOFTWARE ASSURANCE ASSISTANCE

The **Software Assurance Forum** brings public and private stakeholders together to discuss ways to advance software assurance objectives. Through collaborative events, stakeholders raise expectations for product assurance with requisite levels of integrity and security, and promote security methodologies and tools as a normal part of business.

"Build Security In" (BSI) is a collaborative effort to provide tools, guidelines, and other resources, which software developers, architects, and security practitioners can use to build security into software in every phase of development. For information, visit: https://buildsecurityin.us-cert.gov/swa or email software.assurance@dhs.gov.

EXERCISES AND TRAINING

The **CyberStorm Exercise Series** focuses on simulated cyber-specific threat scenarios intended to highlight critical infrastructure interdependence and further integrate Federal, State, international, and private sector response and recovery efforts. The series helps participants assess their response and coordination capabilities specific to a cyber incident. Contact CEP@dhs.gov for more information.

EMERGENCY RESPONSE AND READINESS TEAMS

The **United States Computer Emergency Readiness Team (US-CERT)** operates a 24–7–365 Operations Center; provides situational awareness reports and detection information regarding cyber threats and vulnerabilities and conducts cyber analysis; and provides on-site incident response capabilities to Federal and State agencies. To report suspicious cyber activity, call US-CERT at (888) 828-0870 or email soc@us-cert.gov. The US-CERT's National Cyber Alert System (NCAS) delivers timely and actionable information and threat products, including alerts, bulletins and tips to users of all technical levels. Visit http://www.us-cert.gov/cas/signup.html to subscribe.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) coordinates control systems-related security incidents and information sharing through use of **Fly-Away Teams** with Federal, State, and local agencies and organizations, the intelligence community, the private sector constituents, and international and private sector CERTs. ICS-CERT also operates a **Malware Lab** to analyze vulnerabilities and malware threats to ICS equipment. To report suspicious cyber activity affecting ICS, call the ICS-CERT Watch Floor at (877) 776-7585 or email ics-cert@dhs.gov .

OUTREACH AND AWARENESS

DHS collaborates with its partners, including the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center, to support public outreach and awareness activities, including **National Cyber Security Awareness Month** and the **Stop.Think.Connect.** Campaign. To learn more or to book a speaker for an upcoming event, visit http://www.dhs.gov/cyber or http://www.dhs.gov/stopthinkconnect.

Government Forum of Incident Response and Security (GFIRST) is a Government information-sharing effort focused on daily information exchange among technical operators across the defense, intelligence, law enforcement, and Federal civilian agency communities. The annual **GFIRST National Conference** gathers partners and analysts to share advances in incident response and best practices to strengthen cybersecurity. For more information, visit: http://www.us-cert.gov/gfirst.

Federal Cyber Security Conference and Workshop (FCSCW) is an annual event designed for federal cyber leaders and their support staff to learn and discuss strategies and tactics for securing and defending federal IT systems and networks for trusted and reliable global communication. For more information, email: FNS.SM@fns.gov.

SECURITY REFERENCE ARCHITECTURES

Enterprise Security Reference Architecture development and review services provide agencies with the specialized subject matter expertise needed to develop technical models that will facilitate the deployment of IT services in a cost effective, efficient and consistent manner with minimal risk. The use of standard reference architectures ensures that the cyber security solutions developed by agencies across the federal government will be aligned with national initiatives. Existing Reference Architectures include Trusted Internet Connections, Continuous Monitoring, Wireless Local Area Networks (WLAN), Domain Name System (DNS) Infrastructure, Email Gateway Security, and Telework. In FY12, additional reference architectures will include mobile computing and data protection. For more information on existing reference architectures or to request assistance, contact FNS.NIS@dhs.gov.

CYBERSECURITY STRATEGIC SOURCING

The **Information Systems Security Line of Business (ISSLOB)** is an OMB E-Gov initiative. The ISSLOB facilitates information systems security across government by eliminating duplication of effort and increasing aggregate expertise through the use of Shared Service Centers (SSCs), establishing consolidated acquisitions, and promoting standard practices and lessons learned across agencies. The ISSLOB is currently addressing four common information systems security needs across the government, including: security training, FISMA reporting, continuous monitoring, and Risk Management Framework (RMF) services. For more information, contact FNS.RAS@dhs.gov.